WHAT IS CLAIMED IS:

1. An apparatus for collecting and transmitting biometric data over a network, the apparatus comprised of:

a sensor to collect biometric data; and

a biometric template generator, coupled to the sensor, to convert the biometric data into a biometric template.

2. The apparatus of claim 1, further comprising an output interface, coupled to the biometric template generator, to output the biometric template to a network.

3. The apparatus of claim 1, further comprising a security code generator coupled to the biometric template generator to sign the biometric template.

4. The apparatus of claim 3, wherein the security code generator implements a signing technique using at least one of a key and a token.

5. The apparatus of claim 3, further comprising an output interface, coupled to the biometric template generator, to output the signed biometric template to a network.

6. The apparatus of claim 1, further comprising an image processor coupled between the sensor and the biometric template generator to determine whether the biometric data is suitable for biometric template generation.

7. The apparatus of claim 1, further comprising a biometric matcher to compare a two biometric templates to determine whether the two biometric templates match and to generate a match result.

8. The apparatus of claim 7, wherein the match result is signed.

9. The apparatus of claim 1, further comprising a security module to decrypt and validate a previously enrolled biometric template received via the network.

10. The apparatus of claim 9, wherein the received previously enrolled biometric template is signed, encrypted, and comprises a validation key.

11. A cryptographic system, comprising:

an imaging device for collecting biometric data;

a code generator to generate a digital signature

a key generator to generate at least one key;

a private key storage device coupled to the key generator; and

a public key storage device coupled to the key generator.

12. The system of claim 11, further comprising:

a signature validator to generate a public key; and

an encryptor to encrypt data using the public key; and

a decryptor.

13. The system of claim 11, wherein the key generator comprises logic to create an asymmetric key pair.

14. A method of providing security to biometric data, comprising:

generating a key pair comprising a public key and a private key at an imaging device;

storing the private key in a storage device at the imaging device;

transmitting the public key from the imaging device to a certification authority;

generating an imaging device public key certificate at the certification authority;

generating a certification authority public key certificate at the certification authority; and

transmitting the imaging device public key certificate and the certification authority public key certificate to the imaging device.

15. The method of claim 14, further comprising storing the imaging device public key certificate and the certification authority public key certificate in the storage device at the imaging device.

16. The method of claim 14, further comprising:

generating an asymmetric key pair comprising a public key and a private key at server;

storing the private key in a storage device at the server;

transmitting the public key from the server to a certification authority;

generating a server public key certificate at the certification authority;

generating a second certification authority public key certificate at the certification authority; and

transmitting the server public key certificate and the second certification authority public key certificate to the imaging device.

17. A method of exchanging biometric information between an imaging device and a server, comprising:

authenticating the server at the imaging device;

obtaining a biometric sample at the imaging device;

signing the biometric sample at the imaging device;

generating a data package comprising the biometric sample, a token, the signature, and an imaging device public key certificate;

transmitting the data package to the server;

receiving the data package at the server;

authenticating the imaging device at the server;

validating the signature and the token at the server.

18. The method of claim 17, wherein authenticating the server at the imaging device comprises:

sending a request for a server public key certificate and the token from the imaging device to the server;

generating the token at the server;

retrieving the server public key certificate from a storage device;

transmitting the server public key certificate and the token to the imaging device; and

validating the server public key certificate at the imaging device.

19. The method of claim 18, wherein validating the server public key certificate at the imaging device comprises using a certification authority public key certificate.

20. The method of claim 17, further comprising encrypting the data package using the server public key certificate prior to transmitting the data package to the server, and decrypting the data package at the server.